Teknokultura
Revista de Cultura Digital y Movimientos Sociales

#LEE, A. (2014). A Question of Momentum – Critical Reflections on Individual Options for Surveillance Resistance. *Revista Teknokultura, 11* (2), 425-440.

Recibido: Recibido: 14-05-2014
Aceptado con correcciones: 04-07-2014
Aceptado: 25-07-2014

Link open rewiev:
http://teknokultura.net/index.php/tk/pages/view/opr-216

A Question of Momentum
Critical Reflections on Individual Options for Surveillance Resistance

Una cuestión de Momentum
Reflexiones críticas sobre las opciones individuales de resistencia a la vigilancia

Uma questão de Momentum
Reflexões críticas sobre as opções individuais de resistência à vigilância

Ashlin Lee
School of Social Sciences – University of Tasmania
ashlin.lee@utas.edu.au

ABSTRACT

With the increased visibility of global surveillance systems (such as PRISM) to the public, there have been growing calls for more resistance against surveillance. This article critically engages with the options for resistance suggested by Gary T. Marx (2009), focusing on those that affect the social and material circumstances of individuals, and ignoring the symbolic ones. Through this, the role of technological momentum in global surveillance systems, and

the high cost of resistance for individuals are highlighted. I argue that because of the technological momentum and cost of resistance, many options for resistance are problematic for individuals.

Keywords

Analysis, global surveillance, individuals, technological momentum.

Resumen

Junto con la creciente visibilización pública de los sistemas de vigilancia global (como PRISM), han ido apareciendo cada vez más llamamientos a la resistencia contra este tipo de control. Este artículo analiza críticamente las opciones de resistencia sugeridas por Gary T. Marx (2009), centrándose en las que afectan a las circunstancias sociales y materiales de los individuos, y dejando de lado las que tienen tan solo una dimensión simbólica. A través de este texto se destacan la función del momentum tecnológico en los sistemas de vigilancia global y el elevado coste personal que las resistencia tiene para los individuos. Mi argumento es que debido a estos dos elementos, muchas opciones de resistencia son problemáticas en la dimensión individual.

Palabras Clave

Análisis, momentum tecnológico, individuos, vigilancia global.

Resumo

Junto com a crescente visibilização pública dos sistemas de vigilância global (como PRISM), têm aparecido cada vez mais chamados à resistência contra esta vigilância. Este artigo analisa criticamente as opções de resistência sugeridas por Gary T. Marx (2009), centrando-se nas que afetam as circunstâncias sociais e materiais dos indivíduos, e deixando de lado as que têm tão somente uma dimensão simbólica. Através deste texto se destacam a função do momentum tecnológico nos sistemas de vigilância global e o elevado custo pessoal que as resistências têm para os indivíduos. Meu argumento é que devido a estes dois elementos, muitas opções de resistência são problemáticas na dimensão individual.

Palavras-chave

Análise, vigilância global, indivíduos, impulso tecnológico.

Summary

Sumario

Sumário

Introduction

Edward Snowden and Wikileaks have recently brought discussion on surveillance into the public arena, making startling revelations regarding the existence of global surveillance programs such as PRISM, a state run surveillance system (for more details see The Guardian, 2013). Global surveillance systems are not unusual in contemporary society, routinely used in commerce, security, and communication (Lyon, 2001). These systems however have usually avoided the headlines. With the increased visibility of PRISM and other global surveillance systems, there have been many calls for greater resistance against surveillance.

In this article I critically engage with the idea of resistance, particularly options of resistance available to individuals. Here resistance is conceptualised as those behaviours and actions that seek to change the "dialectic of control" (Giddens, 1984, p. 16) around surveillance in some way, shifting the balance of power between watcher and watched (Lyon, 2007). Of particular interest are those forms of resistance that directly change the social and material circumstances of data collection. Symbolic or passive resistances that don't make these changes are ignored. I contend that many individual options for resistance are problematic. Firstly, because the technological momentum of global surveillance systems like PRISM makes direct and confrontational opposition difficult. Secondly, because the integration of surveillance systems into everyday life makes their disentanglement costly for individuals. I conclude that individual resistance in its current state is problematic, and a broader scope maybe worth considering.

Momentum

The limitations of resistance stem from the asymmetry between surveillance structures and individual forms of resistance, and the accumulation of what Hughes (1994) calls “technological momentum” in surveillance systems. Historian of technology Thomas Hughes argued that technological systems could be thought of like moving physical objects, as gathering forward momentum in their development and adoption (Kirkman, 2004). Momentum is accumulated through forms of capital including favourable social and political networks, and economic resources, that are gathered as systems grow and develop. Successful socio-technical systems

were those that had a great deal of momentum, and therefore resources, behind them to reach their desired goal (Hughes, 1986). Global surveillance can be understood in the same way, as a socio-technical system with great resources invested to increase its momentum. This is clear when the forms of capital involved in global surveillance are considered. This capital refers to both material and economic resources but also social and cultural resources, as no technical system is separate from social contexts (Latour, 2005). Global surveillance systems have been found to have enormous amounts of resources invested. For example, the National Security Agency's (NSA), the creators of PRISM, secret budget for 2013 was in excess of $15 Billion (Braun, 2013). Alongside economic and material support, global surveillance programs were built and justified upon a cultural and political environment (i.e. post 9/11) that was receptive and even welcoming to security and surveillance measures (Monahan, 2010). Any single individual cannot hope to muster resources to combat these kinds of momentum and, as a consequence, individuals face an uphill battle to affect any meaningful resistance to surveillance. Monahan (2006b) argues that this disjunction between individuals and surveillance structures is one of the reasons why resistance occurs. While true, it ignores the implication of technological momentum; that to make an actual change to an individual's surveillance contexts is to also challenge the momentum of the system.

Resistance Options

This is not to suggest that surveillance is a deterministic social phenomena. Surveillance processes are always a consequence of "the context and comportment" (Marx, 2013, p. 5) of any given social situation, with the outcomes of this situation never predetermined. As Gilliom (2005) notes even the most marginalised and disadvantaged members of society can offer forms of resistance to surveillance, challenging the *status quo*. But the question is: do these actions actually change the balance of power and the circumstances of surveillance for individuals? Marx (2003, 2009, p. 297) suggests twelve possible "surveillance neutralisation" techniques for individuals to resist surveillance:

Revista Teknokultura, (2014), Vol. 11 Núm. 2: 425-440
ISSN: 1549 2230

TABLE 1: TWELVE NEUTRALIZATION MOVES

Move	Action
Discovering	Find out if surveillance is in operation, and if it is, where, by whom and how
Avoiding	Choose locations, times periods and means not subject to surveillance
Piggy Backing	Accompany or be attached to a qualifying object
Switching	Transferring an authentic result to someone or thing it does not apply to
Distorting	Altering input such that a technically valid result appears but the inference drawn from it is invalid
Blocking	Eliminating or making data inaccessible
Masking	Involves blocking in that original information is shielded but goes beyond it to involve deception with respect to factors such as identity and location
Breaking	Rendering the surveillance device inoperable
Refusing	"Just say no" – ignore the surveillance and what it is meant to deter
Explaining and contesting	Accounting for an unfavourable result by reframing it in an acceptable way or offering alternative data and the claims of rival experts, making rights claims
Cooperating	Collusive moves with agents
Counter-Surveillance	Role reversal as subjects apply the tactics to agents taking advantage of the double edged potential of tools

Source: Marx, G.T (2009, p.298).

However, in suggesting these surveillance neutralisation devices, Marx (2009) also notes the potential for methods of resistance to be overcome or nullified through appropriate counter-measures taken by the surveillance system or authority. These countermeasures are a function of the momentum of the surveillance system, as momentum dictates the available resources a system has towards its interests. It is for this reason that any individual act of resistance is likely to be easily countered by global surveillance systems – individuals simply lack the

ability to confront and neutralise this momentum. Now consider Marx's typology in this light. His first method of resistance, discovering and raising awareness, is irrelevant as the details of such surveillance systems are already available, and public awareness is at an all time high. These programs still continue. Methods such as refusing surveillance, explaining and contesting surveillance, and co-operating with surveillance do not actively seek to change the circumstances or vulnerabilities of the individual to data collection and are not of interest here. This leaves a set of neutralisation techniques that focus on making changes to the individual's circumstances, including avoiding or breaking surveillance devices, blocking access to personal data, distorting data capture, switching the captured data, and piggy backing onto accepted or unwatched objects or measures. These behaviours represent confrontational forms of resistance in that they directly challenge the socio-material forms of order that allow surveillance to occur. All of these methods are possible for individuals. Personal data may be encrypted to prevent access, and the Internet may be accessed through secure private networks, or routed through services such as TOR that disrupt monitoring (See TOR 2014). This achieves forms of blocking or masking. An individual may choose to enter false data voluntarily, acting as a means of distorting. A user might access the Internet on someone else's computer or use a friend's phone, switching the data collected. Individuals are therefore not without options.

But these options are easily countered by global surveillance systems. The technological momentum, and therefore prior investment and development in global surveillance, means that many of the measures suggested have already been countered by those conducting surveillance. For example, many standard encryption measures, network equipments, and digital devices have vulnerabilities which state authorities are often aware of and exploit at will (Menn, 2013; Riley, 2014; Der Spiegel, 2013). When these approaches do not suffice, state authorities have designed and constructed network infrastructure and hardware to allow direct access to the fibre optic or copper lines themselves (Aron, 2013). Privacy services like TOR have been penetrated by state security services and their encryption protocols broken (Goodin, 2013). Distortion and switching as a form of resistance are also misleading, as they ignore how services like PRISM rely on databases of previously entered information in addition to real time data collection. Entire datasets of personal information are already in the possession of governments and private corporations already (Lyon, 2001). A sudden change in behaviour or shift in the data collected in real time doesn't change prior knowledge, and the analytical and comparative potential of these datasets persists. Data collected and circulated within these databases is notoriously difficult to remove, and is often outside the awareness and means of

individuals themselves (Lyon, 2002). Finally in many cases those conducting surveillance have enormous ranges of extra techniques for collecting personal information. Security organisations in the service of nation states and private companies have a range of covert and exotic measures for data collection (Der Spiegel, 2013), and consumer level surveillance is often built into the many digital infrastructure, networks, and standards that consumers use (Pridmore, 2012). Companies and authorities have also been extraordinarily successful in "seducing" users away from resistance to complicity (Lyon, 2007, p. 102). What this suggests is that for individuals confrontational measures of resistance are limited, and that any meaningful shift in the material realities of data collection is difficult.

The remaining methods of resistance such as avoidance or breaking surveillance infrastructure also present a second problem, a high cost for individual users. While breaking or avoiding surveillance systems are highly successful means of resistance that are difficult to counter, to do these consistently and effectively means abandoning the use of many socio-technical processes that are taken for granted in everyday life in the developed West. I do not suggest that the nation-state (through PRISM or similar programs) is watching your every move, but instead refer to the enormous variety of privately organised and routine surveillance individuals are subject to. For example, data collection while using television (Andrejevic, 2009) and social media (Trottier, 2012), consumer surveillance while shopping in locations such as the supermarket (Coll, 2013), targeted advertising and marketing (Campbell & Carlson, 2002), and continual forms of medical (French & Smith, 2013) and insurance surveillance (Gandy, 1989). While it is easy to consider global surveillance as solely referring to surveillance systems with a global scope (a la PRISM), this obscures the variety of surveillance practices that occur globally. Additionally, many of these systems have enormous practical value, serving as a means to verify the identities of individual citizens, by matching tokens of identity to recorded personal details (Lyon, 2001). Without these systems international travel would be exceedingly difficult, global commerce and financial activities using ATMs or stock exchanges would not be processed (Lyon, 2001), and the provision of state social services such as health and education would be dramatically less efficient and far more costly for individuals and the state (Wood, Ball, Lyon, Norris, & Raab, 2006). Also, although mired in many ethical and social problems, global surveillance networks have contributed towards an increase in security for some nations and their citizens (King, 2013). Resisting surveillance through abandoning services or technologies that make individuals vulnerable is a difficult and personally costly means of resistance that I believe few citizens would actively support, as the non-use of technology has the potential for marginalisation (Warschauer,

2004) and impairs functioning in everyday life (Oudshoorn & Pinch, 2003). Abandoning obvious socio-technical vulnerabilities also does not protect against other surveillance practices like bugging, and doesn't stop previous information about the individual being used.

An individual's options for resistance are therefore limited and problematic. The technological momentum of global surveillance systems means individual actions of resistance are limited and can be countered by surveillance organisers. Other forms of resistance are personally costly for individuals given the entanglement of surveillance in everyday life. I make these points not to suggest that acceptance or resignation are desirable alternatives, or that resistance is not important, but to highlight an unfortunate reality of contemporary surveillance.

Concluding Remarks and Future Directions

Is resistance to global surveillance then pointless for an individual? Perhaps in some current iterations, but that does not mean abandoning resistance is helpful. Global surveillance presents a pressing moral, legal, and social issue for all members of contemporary society. Ignoring surveillance, and allowing global surveillance regimes to go unchallenged and unopposed perpetuates a growing asymmetry between those conducting surveillance and the subject(s) of surveillance. It is therefore important that surveillance and its subsequent asymmetries do not go unquestioned or unopposed, whether this be through resistance or alternative means. But any suggested opposition to surveillance, especially for individuals, needs to recognise the current context of surveillance, including issues of technological momentum and surveillance's role in everyday life, which complicates opposition.

Because of these points, future discussion on resistance, especially for individuals, may benefit from looking beyond confrontational resistance towards ideas more attuned to dealing with the context. One possible angle for this might be considering ideas around how surveillance can be controlled or engaged with, to facilitate a positive outcome for individuals. It is unlikely global surveillance systems will be reversed or halted given the momentum developed so far and the gains these systems have had for those in power. Additionally, this momentum is set to continue to build as a new generation of technologies such as drones (Wall & Monahan, 2011), wearable devices (Whitson, 2013), and algorithmic and intelligent surveillance (Introna & Wood, 2004), are developed and deployed. An individual can never hope to resist, avoid, or destroy all these measures of surveillance. However if Marx's (2013) assertion that surveillance holds no inherent moral character and is contextually determined holds true, then

considering how individuals can engage with surveillance and determine its course could be a good next step. Such an approach would sidestep the idea of confrontation as the basis for resistance, avoiding problems of technological momentum, while acknowledging the role of surveillance in everyday life. Positive change would occur through participation, engagement, and control, instead of fighting, destroying, or hiding from surveillance. This is not an entirely new idea, with Mann (2013) suggesting that all individuals should adopt *veillance* (or watching) technologies to address the current asymmetries of a *sur-veillance* society (where watching occurs only from above). He suggests harnessing the technological momentum of *surveillance* to allow all individuals to watch each other and the authorities. Individual thus do not have to resist *surveillance* when they are able to conduct their own *veillance*, demonstrating how participating and engaging might be positive for individuals. Through this Mann believes that society "will tend to be more balanced, just, prosperous and 'livable'" (Mann, 2013, p. 11), in comparison to where there is *sur-veillance* only. However any such notion of engagement or control would still need to overcome significant hurdles. While new generations of devices, such as Google Glass, may offer a feasible platform for this, there is no guarantee that uptake will be high enough to create a *veillance* society. All individuals need equal access and opportunity to engage for a veillance society to work. As a social measure, it would also require a supportive legislative and political environment, a difficult proposition given that governments and corporations benefit from the current asymmetries. It also begs the question of how individuals would be able to generate enough momentum, whether this be technological, social, political, or economic, to create and maintain such a radical social arrangement.

Consequently, this would mean a shift in focus from individual to group forms of participation and resistance. An obvious counterpoint to much of the above discussion is that it has not engaged with these kinds of group forms of resistance. As Martin, van Brakel, and Burnhard (2009) state resistance to surveillance is best understood as occurring in relation to multiple actors and groups. It has been well demonstrated that it is possible for individual's to come together in collectives or communities to resist or challenge surveillance in these contexts (see Monahan, 2006a). These facts and the necessity to consider groups in the analysis of resistance is not in question, and indeed may offer individuals a way of engaging in resistance. But this should not obscure the fact that surveillance occurs in a world that is increasingly individualised and fragmented (Bauman, 2000) especially for those living in the developed West, and individual options for resistance should still be explored. This article has sought to directly engage with this notion and critique it without at all devaluing or detracting from group options for resistance. Surveillance must be considered as a part of the political eco-

nomic patterns of society (Lyon, 2007), with individualisation existing as an important factor in these patterns. With traditional forms of sociality and community evolving towards an individually directed project (Bauman, 2000), and surveillance being increasingly ubiquitous to these projects (Lyon, 2001), it is left in the individual's hands how this risk is negotiated. Therefore a consideration of the individual and their capacity to act is important and necessary, as it compliments existing understandings of group resistance.

The importance of having options for enacting positive change upon surveillance is enormous, whether these options come from individuals or groups. But any such notion must be pragmatic and open for development. It is hoped this article will encourage further discussion in this vein, for the good of all the subjects under surveillance.

Revista Teknokultura, (2014), Vol. 11 Núm. 2: 425-440
ISSN: 1549 2230

References

ANDREJEVIC, M. (2009). *iSpy: Surveillance and Power in the Interactive Era*. Kansas: University of Kansas Press.

ARON, J. (2013, November 4). NSA Snoops Tech Companies' Fibre-Optic Networks. *New Scientist.* Retrieved from <http://www.newscientist.com/article/dn24519-nsa-snoops-tech-companies-fibreoptic-networks.html>

BAUMAN, Z. (2000). *Liquid modernity*. Cambridge: Polity.

BRAUN, S. (2013, August 29). NSA 'Black Budget' Provides New Details On Surveillance Agency. H*uffintong Post.* Retrieved from <http://www.huffingtonpost.com/2013/08/29/nsa-black-budget_n_3838563.html>

CAMPBELL, J. E., & CARLSON, M. (2002). Panopticon.com: Online Surveillance and the Commodification of Privacy. *Journal of Broadcasting & Electronic Media, 46*(4), 586 - 606.

COLL, S. (2013). Consumption as Biopower: Governing Bodies with Loyalty Cards. *Journal of Consumer Culture, 13*(3), 201-220.

DER SPIEGEL (2013). Interactive Graphic: The NSA's Spy Catalog. Retrieved from <http://www.spiegel.de/international/world/a-941262.html>

FRENCH, M., & SMITH, G. (2013). 'Health' Surveillance: New Modes of Monitoring Bodies, Populations, and Polities. *Critical Public Health, 23*(4), 383-392. doi: 10.1080/09581596.2013.838210

GANDY, O. H. (1989). The Surveillance Society: Information Technology and Bureaucratic Social Control. *Journal of Communication, 39*(3), 61-76.

GIDDENS, A. (1984). *The Constitution of Society: Outline of the Theory of Structuration*. Cambridge: Polity Press.

GILLIOM, J. (2005). Resisting Surveillance. *Social Text, 23*(2 83), 71-83.

GOODIN, D. (2013, September 7). Majority of Tor Crypto Keys Could Be Broken by NSA, Researcher Says. *Ars Technica.* Retrieved from <http://arstechnica.com/security/2013/09/majority-of-tor-crypto-keys-could-be-broken-by-nsa-researcher-says/>

THE GUARDIAN (2013). NSA Files: Decoded. *The Guardian*. Retrieved from <http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1>

HUGHES, T. P. (1994). Technological Momentum. In L. Marx & M. R. Smith (Eds.), *Does technology drive history* (pp. 101 - 114). Cambridge MA: MIT Press.

HUGHES, T. P. (1986). The Seamless Web: Technology, Science, Etcetera, Etcetera. *Social Studies of Science, 16*(2), 281-292. doi: 10.2307/285206

INTRONA, L. D., & Wood, D. (2004). Picturing Algorithmic Surveillance: the Politics of Facial Recognition Systems. *Surveillance & Society, 2*(2/3), 177-198

IRWIN, A. (2001). Constructing the Scientific Citizen: Science and Democracy in the Biosciences. *Public Understanding of Science, 10*(1), 1-18.

KING, R. (2013). NSA Chief Keith Alexander Speaks About PRISM at Black Hat. *Washintong Street Journal - Blogs.* Retrieved from <http://blogs.wsj.com/cio/2013/07/31/general-keith-alexander-speaks-about-prism-at-black-hat/>

KIRKMAN, R. (2004). Technological Momentum and the Ethics of Metropolitan Growth. *Ethics, Place & Environment, 7*(3), 125-139. doi: 10.1080/1366879042000332934

LATOUR, B. (2005). *Reassembling the Social: An Introduction to Actor-Network-Theory*. Oxford: Oxford University Press.

LYON, D. (2001). *Surveillance Society: Monitoring Everyday Life*. New York: McGraw-Hill International.

LYON, D. (2002). *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*. London: Routledge.

LYON, D. (2007). *Surveillance Studies: An Overview*. Cambridge: Polity.

MANN, S. (2013, 27-29th June 2013). *Veilance and Reciprocal Transparency: Surveillance versus Sousveillance, AR Glass, Lifeglogging, and Wearable Computing.* Paper presented at the Technology and Society (ISTAS), 2013 IEEE International Symposium on Technology and Society, Toronto, Canada.

MARTIN, A. K., VAN BRAKEL, R. E., & BERNHARD, D. J. (2009). Understanding Resistance to Digital Surveillance Towards a Multi-Disciplinary, Multi-Actor Framework. *Surveillance & Society, 6*(3), 213 - 232.

MARX, G. T. (2003). A tack in the shoe: Neutralizing and Resisting the New Surveillance. *Journal of Social Issues, 59*(2), 369-390.

MARX, G. T. (2009). A Tack in the Shoe and Taking off the Shoe Neutralization and Counter-neutralization Dynamics. *Surveillance & Society, 6*(3), 294-306.

MARX, G. T. (2013). An Ethics for the New (and Old) Surveillance. In R. S. Francesco FLAMMINI, Giorgio FRANCESCHETTI (Ed.), *Effective Surveillance for Homeland Security: Balancing Technology and Social Issues* (pp. 3 - 20). Boco Ratton: CRC Press.

MENN, J. (2013, December 20). Exclusive: Secret Contract tied NSA and Security Industry Pioneer. *Reuters.* Retrieved from <http://www.reuters.com/article/2013/12/20/us-usa-security-rsa-idUSBRE9BJ1C220131220

MONAHAN, T. (2006a). Counter-surveillance as political intervention? *Social Semiotics, 16*(4), 515-534.

MONAHAN, T. (Ed.). (2006b). *Surveillance and Security: Technological Politics and Power in Everyday Life*. New York: Routledge.

MONAHAN, T. (2010). *Surveillance in the Time of Insecurity*. New Brunswick: Rutgers University Press.

OUDSHOORN, N., & PINCH, T. J. (2003). *How Users Matter: The Co-Construction of Users and Technologies*. Cambridge (MA): MIT press.

PRIDMORE, J. (2012). Consumer Surveillance Context, Perspectives and Concerns in the Personal Information Economy. In K. D. H. Kirstie BALL, and David LYON (Ed.), *Routledge Handbook of Surveillance Studies* (pp. 321 - 329). London: Routledge.

RILEY, M. (2014). NSA Said to Exploit Heartbleed Bug for Intelligence for Years. *Bloomberg News.* Retrieved from <http://www.bloomberg.com/news/2014-04-11/nsa-said-to-have-used-heartbleed-bug-exposing-consumers.html>

TOR. (2014). The TOR Project. Retrieved from <https://www.torproject.org/>

TROTTIER, D. (2012). Interpersonal Surveillance on Social Media. *Canadian Journal of Communication, 37*(2), 319 - 332.

WALL, T., & MONAHAN, T. (2011). Surveillance and Violence from Afar: The Politics of Drones and Liminal Security-Scapes. *Theoretical Criminology, 15*(3), 239-254. doi: 10.1177/1362480610396650

WARSCHAUER, M. (2004). *Technology and Social Inclusion: Rethinking the Digital Divide*. Cambridge (MA): MIT Press.

WHITSON, J. R. (2013). Gaming the Quantified Self. *Surveillance & Society, 11*(1/2), 163-176.

WOOD, D. M., BALL, K., LYON, D., NORRIS, C., & RAAB, C. (Eds.). (2006). Wilmslow: Office of the Information Commissioner.